# PCSRF Conference Call Notes

**Thursday, May 22, 2003 1:30 – 3:30 PM ET**
**Hosted by NIST**

## Participants

Fred Proctor (NIST/MEL)
Keith Stouffer (NIST/MEL)
Joe Falco (NIST/MEL)
Art Griesser (NIST/EEEL)
Mike Fancher (NCMS)
Howard Lipson (Carnegie Mellon – CERT)
Joe Weiss (KEMA)
Nancy Shifflet (Columbia Gas Transmission)
Mike Baker (Honeywell)
Cindy Bickerstaff (Intel)
Dan Carnahan (Rockwell)
Charley Cayot (Applied Solutions Group)
Brad Carlberg (BSC Engineering)
David Kuykendall (Novus)
Jeff Dagle (PNNL)
Kirk Blair (Northeast Utilities)
Tom Good (Dupont)
Tom Phinney (Honeywell)
Joe Dunkle (Boise Corporation)
Dave Teumim (ISA)
Marv Schilt (Rockwell)
Michael McEvilley (DAC)
Nick Weston (Sun)
Dave Saunders (Westin)
Bill Miller (MaCT)

## Purpose

To share status and plans among participants; discuss and get comments on the new Security Capabilities Profile (SCP) for Industrial Control Systems document; plan the timing, location and agenda for the next face-to-face meeting.

## Web Site Updates

All information on the PCSRF site is password protected. If you don't have a username and password yet, please follow the directions located at http://www.isd.mel.nist.gov/projects/processcontrol/members.html to request one.

The following documents were added to the PCSRF web site:

Security Capabilities Profile for Industrial Control Systems Document -
http://www.isd.mel.nist.gov/projects/processcontrol/members/documents/ICS-8-May.doc

NIST Cybersecurity of Industrial Control Systems Testbed Presentation ISA - January 23, 2003 -
http://www.isd.mel.nist.gov/projects/processcontrol/members/documents/Presentations/ISA-23-Jan-2003.ppt

NIST Process Control Security Testbed -
http://www.isd.mel.nist.gov/projects/processcontrol/members/documents/Equipment_list_small.ppt

Categorization of Vulnerabilities - Pipeline Sector Security Meeting -
http://www.isd.mel.nist.gov/projects/processcontrol/members/documents/pipeline.doc

Categorization of Vulnerabilities - Chemical Sector Security Meeting -
http://www.isd.mel.nist.gov/projects/processcontrol/members/documents/chemical_vulnerabilites.doc

Chemical Sector - Security Objectives -
http://www.isd.mel.nist.gov/projects/processcontrol/members/documents/chemical_objectives.doc

Categorization of Vulnerabilities - Discrete Manufacturing Security Meeting -
http://www.isd.mel.nist.gov/projects/processcontrol/members/documents/manufacturing_vulnerabilites.doc

Discrete Manufacturing Requirements -
http://www.isd.mel.nist.gov/projects/processcontrol/members/documents/manufacturing_requirements.doc

## NIST updates

Keith Stouffer (NIST/MEL) reported that PCSRF now has approximately 250 – 280 registered members (about 10% are active members.)

There have been two additional sector specific workshops to address vulnerabilities and security objectives:

- Pipeline sector (API) – held in Houston – Michael McEvilley attended (January 2003)
- Chemical sector – held at NIST (January 2003)

Information gathered from the sector specific workshops (oil -API, chemical, and discrete parts - NCMS) has been incorporated into the SPS document.

Michael McEvilley (DAC) has revised and reorganized the SPS into a new document

- Renamed to "Security Capabilities Profile (SCP) for Industrial Control Systems"
- Includes info from the sector specific workshops (discrete parts, oil, chemical)
- Softened the text throughout to be less "security-ease"
- Added a section on how this document fits with various efforts (PCSRF, SP99, NIAP and other industry specific initiatives) and a diagram was included to illustrate the process within which this document fits.
- Added functional implementation requirements and assurance verification requirements

We would like to thank Bill Miller, Dale Peterson, Tom Good, Eric Cosman, Mark Heard, Dave Teumim and others for early comments that helped shape the new Security Capabilities Profile for Industrial Control Systems document.

NIST has initiated the development of a security testbed comprised of several implementations of typical industrial control and networking equipment as well as relevant sensors and actuators. This industrial control security testbed is being used at NIST to develop test methods for validation and conformance testing of security implementations. The testbed is also being used to help identify system vulnerabilities as well as establish best practice guidelines.

Information about the NIST testbed was presented at the ISA Control System Security Conference on January 23, 2203 in Houston. The presentation is available on the PCSRF site: http://www.isd.mel.nist.gov/projects/processcontrol/members/documents/Presentations/ISA-23-Jan-2003.ppt

Bill Miller and Persistent Systems (developers of WaveRelay wireless security), visited the NIST testbed and discussed possible collaboration efforts.

We would like to have the next face-to-face meeting ASAP so that we can discuss and resolve any issues with the new Security Capabilities Profile for Industrial Control Systems document and determine possible scopes for the Protection Profiles that will be generated from the Security Capabilities document.

Joe Falco (NIST/MEL) reported additional information on the NIST testbed. There is a Power Point slide of the testbed available on the PCSRF site:
http://www.isd.mel.nist.gov/projects/processcontrol/members/documents/Equipment_list_small.ppt

The testbed contains:

- Network hardware (firewalls, router, wireless access point, switches, modems, etc.)
- Industrial equipment (several PLCs and a DeltaV system)
- Flow meters, pumps, ultrasonic level sensors
- Conveyor system with DeviceNet

The testbed is being used at NIST to develop test methods for validation and conformance testing of security implementations. The testbed is also being used to help identify system vulnerabilities as well as establish best practice guidelines. NIST is looking for testable hardware.

Art Griesser (NIST/EEEL) reported that with the EEEL testbed they are measuring the performance impact of adding encryption to SCADA links.

## Round table status updates

Jeff Dagle (PNNL) reported that there is a DOE RFP for cybersecurity of process controls. Proposals are due by the end of July. Jeff sent info on this RFP to the PCSRF email list.

Howard Lipson (Carnegie Mellon – CERT) reported that he is new to the group and has been a security researcher for the past 12 years and is now with Carnegie Electric Industry Center (CEIC).

Mike Fancher (NCMS) reported that NCMS is forming a project with the Big 3 automakers for shop floor security. The group was formed over the winter and should become active this summer.

Joe Weiss (KEMA) reported on the ongoing parallel efforts among the National Labs and that are several standards committees being formed (SP99, IEEE, IEC, etc.). There is an ANSI meeting June 9-10. Joe suggested that PCSRF act as the central coordinator for these efforts. Next KEMA conference is in November at NIST.

Joe Dunkle (Boise Corporation) reported that he is working with a technology audit group for developing corporate policy for pulp and paper.

Dave Teumim (ISA) reported that there will be an ISA Industrial Network Security conference in Houston October 21 – 23, 2003. There will be an SP99 meeting on October 23. Dave is working in TR3 for testing, audits and metrics.

Tom Good (Dupont) suggested that PCSRF should address where it is going with documents, timing and deliverables and audience. He asked who is going to use the document and suggested that the Common Criteria is difficult and may not be suitable for the audience. Tom also suggested that we talk to suppliers and respond to their need.

Dan Carnahan (Rockwell) seconded Tom Good's proposal. Seems like a lot of the responsibility falls on the user of the control systems. If these efforts are targeted toward suppliers, then we must communicate with suppliers. Safety also complicates things; how to by-pass security when safety is an issue.

Bill Miller (MaCT) reported on a new web-server Protection Profile. He sent email on this to the PCSRF list. The info can be found here: http://www.iatf.net/protection_profiles/single_level_web.cfm
Bill suggested that we compare this document to the SCP document. At the Toronto ISA show there was a demo of security enabled advanced wireless technology. Bill is putting together an introduction to the Common Criteria online course. The course will be made available to PCSRF participants at no cost. Fred Proctor added that education is necessary but not sufficient; we cannot simply put of PPs and say we are done.

David Kuykendall (Novus) reported on Java–enabled network security devices that they are working on.

Charley Cayot (Applied Solutions Group) suggested that we should specify a period for evaluation in the SCP document. Need to put meat into the component level so that response can be faster than 3-5 year cycle. The SCP document should be consistent with other NIST documents for risk assessment and evaluation.

Joe Weiss added that NERC states that every year we redo certification. FERC is saying the NERC should set the standards. NERC includes the control center only – not SCADA, RTU, etc.

Michael McEvilley (DAC) reported on his background. He reiterated his stance that the Common Criteria is relevant to this effort. The primary focus for the revisions to the SPS document was to address the unfamiliarity with the CC. If we are serious about measuring conformance, we need the CC concepts. There are no mandated regulations for cybersecurity – we can't say that we need 3 or 5 year recertification. SCP renaming suggests highest level of abstraction – we now need to drill down. Michael is also looking at IEC 61508 (safety standard). 61508 states " you will have SW development process; you will have revision control."

Dan Carnahan added that IEC 61511 and 62026 are sector specific extensions to 61508. They are still high level, but focused on domain. 61508 is too broad to be applied easily.

Dave Teumim added in SP99, they are using the V-model safety lifecycle model from IEC 61508.

Michael McEvilley added that if you replace "safety" with "security" in 61508, that's the SCP document. Michael also asked advise from the group on case histories, etc. that would help us with the SCP and PP.

Dave Teumim suggested that we discuss the relationships of the related efforts (SP99, IEC, etc.) during the next face-to-face meeting and that a graphical representation would really help. When SP99 introduced the V-model, it crystallized the discussion and roadmap.

Tom Phinney added that authentication has to be performed for safety as well as security.

Bill Miller suggested some PP candidates: Web server HMI and firewall. He also suggested that we should look at IATF PPs as examples for our work.

## Next face-to-face meeting

We would like to have the next face-to-face meeting ASAP so that we can discuss and resolve any issues with the new Security Capabilities Profile for Industrial Control Systems document and determine possible scopes for the Protection Profiles that will be generated from the Security Capabilities document.

The proposal is for a one-day meeting, either the week of June 9 or the week of June 16. The meeting will be held at NIST in Gaithersburg, Maryland. If you would like to attend the next PCSRF face-to-face meeting, please send an email to stouffer@cme.nist.gov with the dates that you are available by Wednesday, May 28. I will send an email with the selected date of the meeting COB on May 28.

On May 9, I also talked with Joe Bergman from the Open Group and he offered us space for a PCSRF meeting at their meeting on July 22 in Boston. IEEE will be there as well.